List-Decoding of Parity-Sharing Reed-Solomon Codes in Magnetic Recording Systems

Michael K. Cheng and Paul H. Siegel
Center for Magnetic Recording Research, University of California, San Diego, La Jolla, CA 92093-0401

Abstract— **An (n, k) Reed-Solomon (RS) code is used in a magnetic recording system to help reduce the Word Failure Rate (WFR). If the channel Signal-to-Noise Ratio (SNR) exceeds a certain value, the full power of a given RS code may be needed only on a few occasions to guarantee a target WFR. When this occurs, a parity-sharing scheme can be used to group a number of RS codewords into a larger codeword block. The target WFR can, therefore, be achieved at a higher code rate. An efficient list-decoding technique has recently been developed by Guruswami and Sudan (G-S) that allows error correction beyond the classical "half-the-minimum-distance" bound. Koetter and Vardy (K-V) have further extended the G-S algorithm to perform soft-decision list-decoding. This work will show that G-S hard-decision and K-V soft-decision list-decoding of parity-sharing codes are both effective and computationally manageable schemes on the discrete memoryless and partial response channels.**

I. Introduction

A Reed-Solomon code can be designed to meet a target Word Failure Rate (WFR) on a discrete memoryless channel (DMC) that experiences independent symbol errors with probability p. A WFR is defined to be the rate at which the RS decoder is unable to find the correct codeword. If a long RS code is used with this channel, then a codeword will, with high probability, experience a typical number of errors e [1], [2, Ch 3.]. Therefore, the number of parities required to achieve a target WFR approaches $2e$ from above with increasing code length. To guarantee a target WFR with a practical code length, we will require the number of parities to be greater than $2e$ because from time to time, a codeword may experience more than the expected number of symbol errors. However, when we group a number of codewords together, it is unlikely that many of the codewords in the group will have experienced more than the average number of symbol errors at the same time. This observation leads to the opportunity for parity sharing because we can use the corrected codewords to help us recover the codewords that encountered more than the usual number of symbol errors.

This work deals with list-decoding of parity-sharing RS codes for use on the DMC and partial response (PR) channels. In Section II, we illustrate the construction and decoding approach of a two-level parity-sharing block. The code structure requires that the codewords be systematically encoded. In Section III, we discuss how to obtain a systematic generator matrix for a generalized Reed-Solomon code. In Section IV, we provide the concepts behind the G-S and K-V algorithms and show that list-decoding can be extended to treat both errors and erasures. In Section V, we present the decoding analysis of the two-level parity-sharing RS codes on both the DMC and the PR channels. We give a technique to calculate the average WFR that can assist in code design. In Section VI, we verify our analysis through simulations and demonstrate the efficacy of parity-sharing codes.

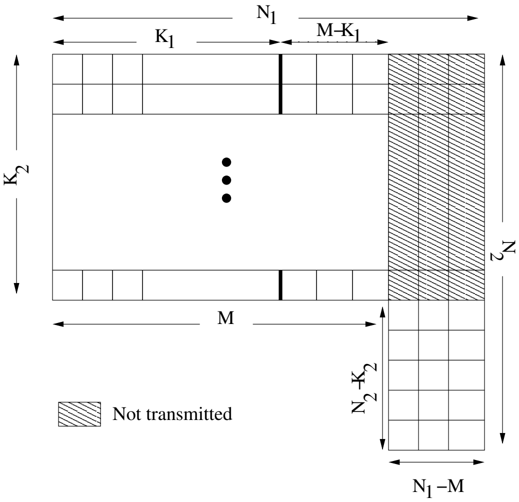

Fig. 1. Construction of an (N_1, K_1), (N_2, K_2) parity-sharing RS code.

II. Two-level Parity-Sharing Reed-Solomon codes

A. Constructing a two-level parity-sharing RS code

A two-level parity-sharing RS code can be constructed in a fashion similar to a product code; that is, we stack a group of K_2 systematic (N_1, K_1) RS codewords together and re-encode the last $N_1 - M$ columns using an (N_2, K_2) systematic RS code. However, only the first M symbols of each row codeword and the $(N_1 - M) \times (N_2 - K_2)$ shared-parities are transmitted over the channel as illustrated in Fig. 1. The rate of the parity-sharing code is $\frac{K_1 K_2}{K_2 M + (N_1 - M)(N_2 - K_2)}$ and a rate gain can be achieved if $N_2 < 2K_2$. We can continue in this way to build higher level parity-sharing codes. A general construction can be found in [3].

B. Decoding of the two-level parity-sharing RS code

The two-level parity-sharing RS code is decoded in a turbo-like approach, shown in Fig. 2. The row codewords are first errors-and-erasures decoded to correct any erroneous symbols and fill in the untransmitted symbols. The $(N_1 - M)$ column codewords are then errors-and-erasures decoded to try to correct any errors in the shared parities and fill in the missing symbols that could not be decoded in the first row pass. Finally, the rows are errors-and-erasures decoded again to fill in any remaining parities and recover the original codewords.

This work was supported by the Information Storage Industry Consortium (INSIC) and by the Center for Magnetic Recording Research (CMRR), University of California San Diego.

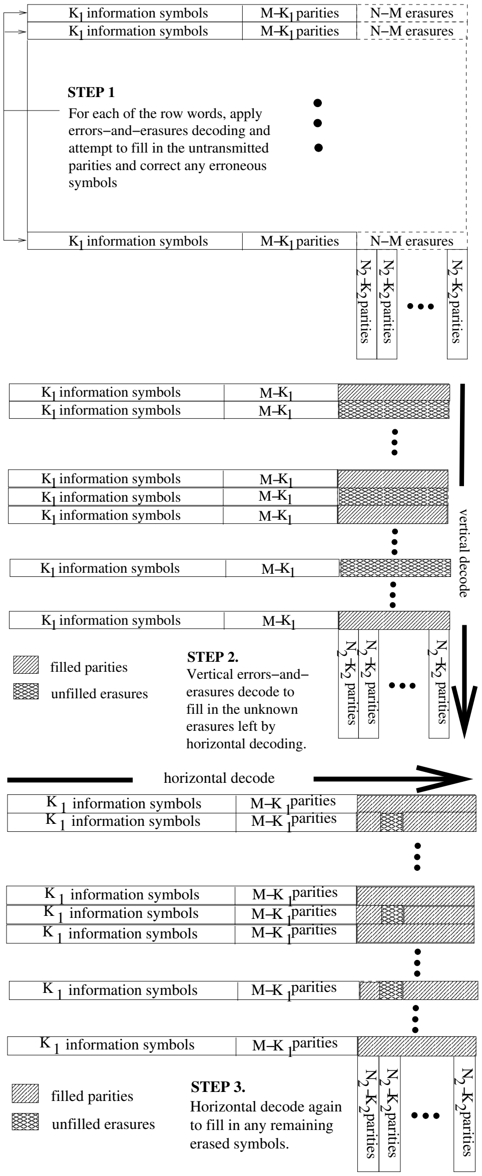

Fig. 2. Steps to decode a parity-sharing RS code

III. Systematic Encoding of Generalized Reed-Solomon codes

The two-level parity-sharing scheme requires systematic encoding of the information block. Columnwise decoding of the parity-sharing code (STEP 2, Fig. 2) assumes that parities of the row code are the information words of the column code. Without systematic column encoding, the row parities would be mapped to some other symbols during column encoding. Row decoding attempts to fill in the information portion of the column words with row parities. These recovered symbols would not match the codeword symbols produced by a nonsystematic column code and column decoding could not proceed.

Our work explores the effects of list-decoding parity-sharing codes; therefore, we need to consider the definition of Reed-Solomon codes used by the G-S and K-V decoding algorithms.

Definition 1: An (n, k) Generalized Reed-Solomon (GRS) code over a finite field $\mathbb{F}_q$ is defined as

$$\mathbb{C}_{RS(n,k)} = \left\{ \left(f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_n)\right) \mid f(x) \in \mathbb{F}_q^{k-1}[x] \right\}$$

where $\mathbb{F}_q^{k-1}[x]$ indicates the ring of polynomials in x with degrees less than k and α_i's are n distinct non-zero elements of the field.

To construct a parity-sharing code based upon GRS component codes, we need a systematic generator matrix G_{sys}. A generator matrix for the GRS code that is suggested by Definition 1 can be obtained by taking a set of k basis polynomials that span $\mathbb{F}_q^{k-1}[x]$ and evaluating each polynomial at the code locators α_i. For example, the matrix corresponding to the basis $\{1, x, x^2, \cdots, x^{k-1}\}$ is

$$G_{ev} = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{n-1}^2 & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_{n-1}^{k-1} & \alpha_n^{k-1} \end{bmatrix}$$

A generator matrix can be put in systematic form by row and column operations; equivalently, there exists a transformation matrix T of size $k \times k$ such that the matrix G_{sys} defined by

$$G_{sys} = T \cdot G_{ev}$$

is systematic.

To find T, we note that the expression for G_{sys} can be expanded as

$$\begin{aligned} G_{sys} &= T \cdot G_{ev} \\ &= T \cdot \left[A_{k\times k} \mid B_{k\times(n-k)}\right] \\ &= \left[T_{k\times k} \cdot A_{k\times k} \mid T_{k\times k} \cdot B_{k\times(n-k)}\right] \\ &= \left[I_{k\times k} \mid P_{k\times(n-k)}\right]. \end{aligned}$$

Since A is a Vandermonde matrix and therefore invertible, we can write

$$T = A^{-1}$$

and set $P_{k\times(n-k)} = A^{-1}B_{k\times(n-k)}$.

IV. List-Decoding

A. The Guruswami-Sudan (G-S) algorithm

Guruswami and Sudan developed a polynomial-time list-decoding algorithm by using bivariate polynomial interpolation [4]. Given a received word $\underline{y} = (y_1, y_2, \cdots, y_n)$ and the list of code locators $\underline{x} = (x_1, x_2, \cdots, x_n)$, where $y_i \in \mathbb{F}_q$ and $x_i \in \mathbb{F}_q \setminus \{0\}$, the G-S algorithm generates a set of n coordinates and attempts to find a polynomial $Q(x, y)$ that fits each coordinate pair (x_i, y_i) with a multiplicity of m. The y-roots of $Q(x, y)$ are the candidate codeword polynomials. The algorithm can correct up to $\tau < n - \sqrt{n(k-1)}$ errors, exceeding the classical bound. The multiplicity required to correct τ errors is calculated as $m = 1 + \left\lfloor \frac{(k-1)n + \sqrt{((k-1)n)^2 + 4\left((n-\tau)^2 - (k-1)n\right)}}{2\left((n-\tau)^2 - (k-1)n\right)} \right\rfloor$.

The G-S algorithm can also be viewed as finding a polynomial that interpolates a $q \times n$ matrix $\mathbf{M}$ with each $(i, j)^{th}$

Algorithm 1 The List-Decoding algorithm [4], [7]

```
Inputs: $n$, $k$, $q$ and a size $q \times n$ interpolating matrix $\mathbf{M}$
  1) Interpolate with multiplicity. Find a bivariate polynomial $Q(x,y)$ with minimum $(1, k-1)$ weighted degree that passes through the nonzero entries $(i,j)$ of $\mathbf{M}$ with a zero of multiplicity $m_{i,j}$.
  2) Factor $Q(x,y)$ into $y$-roots.
Output: The set of $y$-roots is the list of candidate codeword polynomials.
```

entry marked by a non-negative integer $m_{i,j}$. This interpolating matrix has one non-zero entry, with the value m, in each column. The non-zero entry in column j is in row i, where $y_j = \alpha_i$. Algorithm 1 is then applied to find the list of candidate codewords. Efficient methods for bivariate polynomial interpolation and factorization can be found in [5] and [6], respectively.

B. The Koetter-Vardy algorithm

Koetter and Vardy developed a technique that uses channel observations to derive an interpolating matrix $\mathbf{M}$. Algorithm A [5], [7] takes as input a size $q \times n$ reliability matrix $\mathbf{\Pi}$ provided by the channel and uses this soft information to recursively find an $\mathbf{M}$ that would maximize the inner product $\langle \mathbf{\Pi}, \mathbf{M} \rangle$. The K-V algorithm produces a multiplicity matrix $\mathbf{M}$ that may have more than one nonzero entry per column. Once $\mathbf{M}$ is found, Algorithm 1 is used to generate the list of codewords. The flexibility in multiplicity allocation allows the K-V algorithm to obtain a better performance and complexity tradeoff than the G-S algorithm.

C. List errors-and-erasures decoding

The G-S and K-V algorithms can be used for list errors-and-erasures decoding. In the G-S algorithm, we simply set the columns of $\mathbf{M}$ corresponding to the erased positions to the all-zeros vector. For a received word with s erasures, the G-S algorithm can correct up to $\tau(s) < (n-s) - \sqrt{(n-s)(k-1)}$ errors [4]. In the K-V algorithm, we can set the columns of $\mathbf{\Pi}$ corresponding to the erased positions to the uniform probability vector $\left[\frac{1}{q}, \cdots, \frac{1}{q}\right]^T$ and run Algorithm A to obtain an interpolating matrix $\mathbf{M}$. In each of these cases, we apply Algorithm 1 to $\mathbf{M}$ and calculate the candidate codewords.

V. Decoder Analysis

A. The Discrete Memoryless Channel (DMC)

We present the decoder analysis for the parity-sharing scheme on the DMC. Our approach is based on that proposed by Collins [1], but we elaborate on the discussion in [1] and extend the analysis to list-decoding of parity-sharing codes. The two-level parity-sharing code parameters are indicated in Fig. 1. We introduce the term μ to be used to reduce the vertical decoding miscorrection probability, i.e, when $\mu+2$ erasures are observed in any vertical word, no further decoding attempts of the component codewords will be made and a decoding failure would be declared for the entire parity-sharing block.

We denote by $E_n(p,l)$ the probability of having l or more symbol errors in a length-n word, where the symbol error probability is p. Then we can write

$$E_n(p,l) = 1 - \sum_{i=0}^{l-1} \binom{n}{i} p^i (1-p)^{n-i}. \tag{1}$$

For the two-level parity-sharing scheme, the probability that a horizontal codeword fails to decode when all vertical codewords fail is given by

$$G_\infty = E_M(p, t+1). \tag{2}$$

The error decoding radius of the punctured horizontal codeword is $t = \left\lfloor \frac{M-K_1}{2} \right\rfloor$. The probability of exactly i horizontal failures among all the horizontal codewords except the first is given by

$$F_i = \binom{K_2-1}{i} G_\infty^i (1-G_\infty)^{K_2-1-i}. \tag{3}$$

We define $t(u) = \left\lfloor \frac{N_1-K_1-u}{2} \right\rfloor$ and $t(i) = \left\lfloor \frac{N_2-K_2-i}{2} \right\rfloor$. The probability that a vertical decoding fails given there are i horizontal erasures is denoted $p_{vfail}^{(i)}$ and expressed as

$$p_{vfail}^{(i)} = \sum_{j=t(i)+1}^{N_2-K_2} \binom{N_2-K_2}{j} p^j (1-p)^{N_2-K_2-j}. \tag{4}$$

The probability that the first horizontal codeword cannot decode given there are i erasures in the information symbols of the vertical codewords is

$$\begin{aligned} G_i &= \sum_{u=0}^{N_1-M} \binom{N_1-M}{u} \left(p_{vfail}^{(i)}\right)^u \left(1-p_{vfail}^{(i)}\right)^{N_1-M-u} \\ &\quad \cdot \sum_{v=t(u)+1}^{M} \binom{M}{v} p^v (1-p)^{M-v}. \end{aligned} \tag{5}$$

The decoder failure rate (DFR) as shown in [1] is

$$DFR = \sum_{i=0}^{K_2-1} F_i G_i \tag{6}$$

and can be bounded as

$$\begin{aligned} \sum_{i=0}^{K_2-1} F_i G_i &\le G_\mu \sum_{i=0}^{\mu} F_i + G_\infty \sum_{i=\mu+1}^{K_2-1} F_i & (7) \\ &\le G_\mu + G_\infty \sum_{i=\mu+1}^{K_2-1} F_i. & (8) \end{aligned}$$

The bounds in (7) and (8) follow from the fact that most of the probability mass of F_i lies in the first μ terms.

The same analysis can be extended to G-S list-decoding. We replace t in (2) by $\tau = M - \sqrt{M(K_1-1)}$, $t(i)$ in (4) by $t(i) = (N_2-i) - \sqrt{(N_2-i)(K_2-1)}$ and $t(u)$ in (5) by $t(u) = (N_1-u) - \sqrt{(N_1-u)(K_1-1)}$.

B. Word Failure Rate analysis

Let $\overline{N}_f$ be the average number of horizontal word failures when a parity-sharing block fails to decode. Then

$$\overline{N}_f = 1 + (K_2 - 1)\, G_\infty \tag{9}$$

because there is at least one horizontal word that failed and each of the remaining $(K_2 - 1)$ words will experience an independent failure probability of G_∞. The average word failure rate (WFR) can be bounded as

$$\begin{aligned} \overline{WFR} &= \overline{N}_f \cdot \sum_{i=0}^{K_2-1} F_i G_i \\ &\leq \overline{N}_f \left(G_\mu + G_\infty \sum_{i=\mu+1}^{K_2-1} F_i \right). \end{aligned} \tag{10}$$

C. The Partial Response (PR) channel

We can predict the performance of parity-sharing RS codes on PR channels with AWGN by employing the technique developed by Weathers, *et. al.,* [8] to estimate the symbol error rate. Letting $d^2(\lambda)$ be the squared distance of an error event λ, D^* be the set of all possible $d(\lambda)$ and σ^2 be the noise variance, then

$$Pr\,(\text{bit error}) \leq \sum_{d \in D^*} N_d \cdot Q\left(\frac{d}{2\sigma}\right). \tag{11}$$

Assuming there are l bits per symbol and that bit errors are independent, then

$$Pr\,(\text{symbol error}) \leq 1 - (1 - Pr\,(\text{bit error}))^l. \tag{12}$$

For a given channel SNR and σ, we can calculate the symbol error probability and use this value in the analysis developed for the DMC in Section V-A to bound the decoder performance on PR channels. The symbol-based BCJR algorithm [9] is used to decode the PR channel and a symbolwise block interleaver is used to distribute the correlated errors. Furthermore, if we do not hard-limit the symbol-based BCJR output, we can apply K-V list-decoding to the parity-sharing code blocks.

VI. Results

Using the analysis developed in Section V we plot the performance of parity-sharing codes. For the DMC, we use the code parameters $N_1 = N_2 = 255$, $K_1 = K_2 = 223$, $M = 239$, and $\mu = 27$. The result is given in Fig. 3. We compare decoding of the base $RS\,(255, 223)$ code versus the parity-sharing scheme and note that both the classical and (G-S) list-decoding curves cross at high values of $1 - Pr\,(\text{symbol})$. This observation confirms that when the probability of symbol errors is small enough, the parity-sharing code can exceed the performance of the base RS code, with a 5.68% rate advantage obtained by sharing parities. We also compare the list-decoding curve to the classical decoding curve and note that, just as in the base case, benefits also result in list-decoding of parity-sharing codes.

To verify our analytical bounds, we simulated the performance of classical and list-decoding for the parity-sharing code. To save simulation time, the G-S curve is obtained using a threshold approach [9] and a decoding attempt is declared successful as long as the correct codeword is in the list. It is impractical to run a long simulation to obtain the WFRs at the intersection points predicted by analysis, but for an obtainable WFR region we see in Fig. 4 that the analytical calculation does, in fact, upper bound the simulated performance.

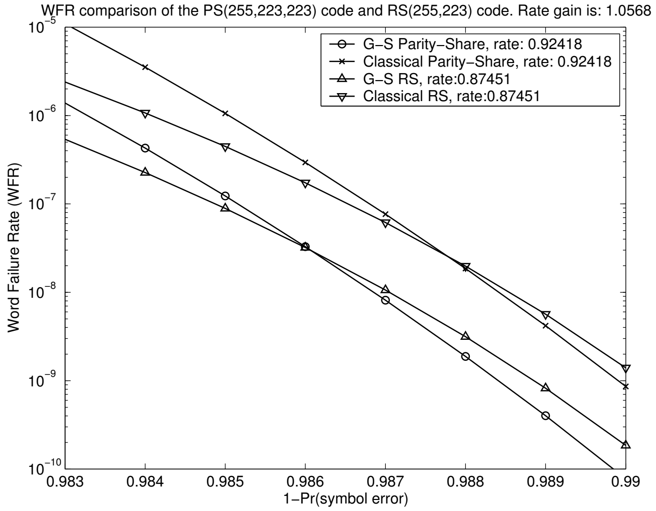

Fig. 3. WFR comparison on the DMC obtained by equation (10).

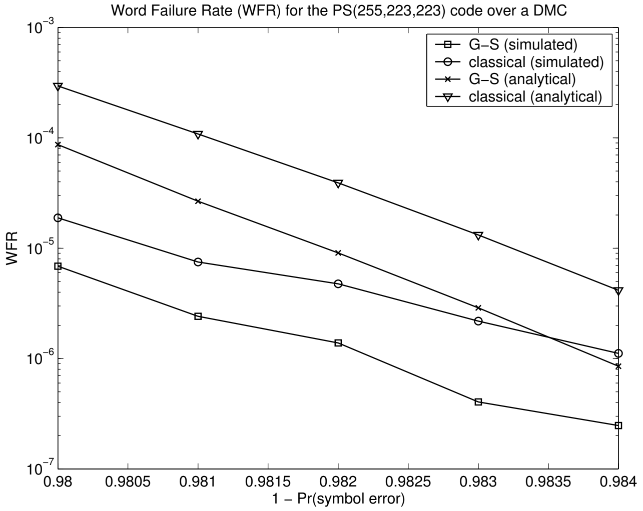

Fig. 4. Simulated decoding performance on the DMC

For the EPR4 channel with transfer function $h(D) = (1 - D)(1 + D)^2$, we use the code parameters $N_1 = N_2 = 31$, $K_1 = 26$, $K_2 = 21$, $M = 29$, and $\mu = 5$ to generate results in a reasonable amount of simulation time. We expect the simulated decoding behaviour and gain to extend to codes over larger fields. The analytical bound is given in Fig. 5. We see that the parity-sharing code achieves a lower WFR than the base RS code at an SNR above 8.1 dB using classical decoding and at an SNR above 7.4 dB using (G-S) list-decoding. It becomes advantageous to use the parity-sharing scheme at SNRs beyond these cross points due to a 3.5% code rate gain. The simulated performance is shown in Fig. 6. Threshold conditions are used

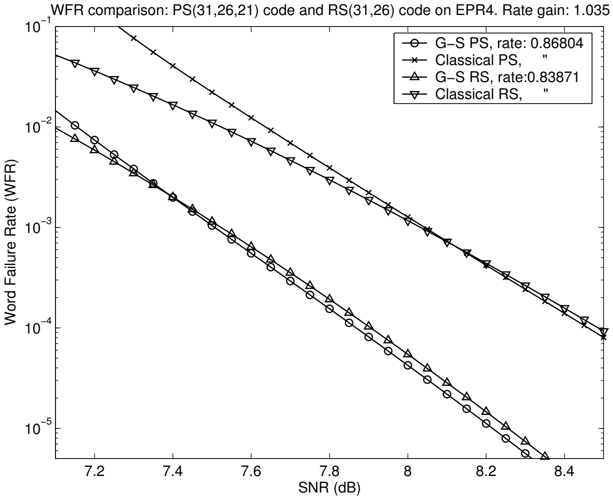

Fig. 5. The analytical performance of $(31, 26, 21)$ parity-sharing scheme over $GF\,(32)$ on the EPR4 channel.

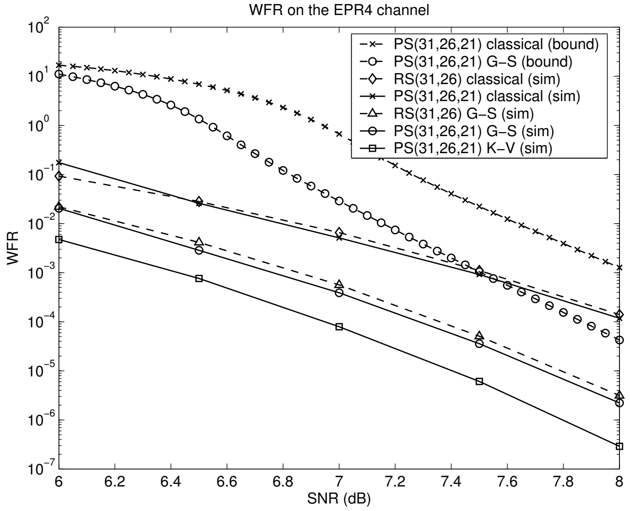

Fig. 6. Simulated decoding performance on the EPR4 channel. The number of interpolation points used by K-V decoding is $S = 50 \cdot N_1$.

to generate the curves for both G-S and K-V list-decodings. The analytical bounds are marked by the top two curves. We note that the bounds are loose when compared to the simulated results. This is due to the fact that we overestimate the symbol error rates when using the union bound especially at low SNRs; nonetheless, our method provides a tool to compare the relative performance of parity-sharing codes on PR channels and allows us to select the code parameters according to the design requirements. We also compare the simulated WFR of the conventional $RS\,(31, 26)$ to the parity-sharing $PS\,(31, 26, 21)$ code. We see, just as predicted by analysis, that the parity-sharing scheme achieves a lower WFR at a higher code rate in both classical and G-S decoding. We also observe that K-V soft-decision decoding of the parity-sharing code provides an additional 0.5 dB gain over G-S decoding. The cost of using parity-sharing codes is the extra computations required to encode and decode the vertical codewords. Although not included here, we have results that indicate a reduced WFR can also be obtained by applying list-decoding to only the vertical codewords. The analytical and simulated results affirm that list-decoding of parity-sharing codes is an effective scheme that can tradeoff performance with computational complexity.

VII. Summary

The performance of block codes improves with codeword length. For RS codes, the length is constrained by the size of the field over which the code is defined. The computation and memory required to carry out Galois field arithmetic increase with field size and therefore, decoding a long RS code can be impractical. For a channel with a high SNR, parity-sharing codes can be used to obtain the performance advantages of a long block code, but with acceptable complexity. In this paper, we presented a two-level parity-sharing RS code and discussed its construction and decoding techniques. The parity-sharing scheme requires systematic encoding of the component codewords. We, thus, provided a simple method of finding the systematic generator matrix for a generalized RS code. We reviewed the G-S and K-V list-decoding algorithms, and showed that they can be used in list errors-and-erasures decoding. We then calculated upper bounds on the WFR when applying classical decoding and the G-S list-decoding to parity-sharing codes over the DMC and PR channels. Our bounds demonstrated that parity-sharing codes can exceed the performance of conventional RS codes at high channel SNRs while obtaining a higher code rate. We also observed that G-S list-decoding of parity-sharing codes can lead to a lower WFR versus classical decoding, just as in the case of conventional RS codes. Moreover, the WFR can be reduced further by applying the K-V soft-decision decoding algorithm. Through simulations, we verified that our bounds on the WFRs are good indicators of relative performance and can assist in code design. List-decoding of parity-sharing codes is a potentially attractive scheme for use in magnetic recording systems.

References

[1] O. M. Collins, “Exploiting the cannibalistic traits of Reed-Solomon codes,” *IEEE Trans. Commun.*, vol. 43, no. 11, pp. 2696–2703, Nov. 1995.

[2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley, 1991.

[3] K. Abdel-Ghaffar and M. Hassner, “Multilevel error-control codes for data storage channels,” *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 735–741, May 1991.

[4] V. Guruswami and M. Sudan, “Improved decoding of Reed-Solomon and Algebraic-Geometry codes,” *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1757–1767, Sept. 1999.

[5] W. J. Gross, F. R. Kschischang, R. Koetter, and P. G. Gulak, “A VLSI architecture for interpolation in soft-decision list-decoding of Reed-Solomon codes,” in *Proceedings of the 2002 IEEE Workshop on Signal Processing Systems*, San Diego, CA, Oct. 2002, IEEE, pp. 39–44.

[6] R. M. Roth and G. Ruckenstein, “Efficient decoding of Reed-Solomon codes beyond half the minimum distance,” *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 246–257, Jan. 2000.

[7] R. Koetter and A. Vardy, “Algebraic soft-decision decoding of Reed-Solomon codes,” in *Proc. IEEE Int. Symp. Information Theory*, Sorrento, Italy, June 2000, IEEE, p. 61.

[8] A. D. Weathers, S. A. Altekar, and J. K. Wolf, “Distance spectra for PRML channels,” *IEEE Trans. Magn.*, vol. 33, no. 5, pp. 2809–2811, Sept. 1997.

[9] M. K. Cheng, J. Campello, and P. H. Siegel, “Soft-decision Reed-Solomon decoding on partial response channels,” in *Proc. IEEE Global Telecom. Conf.*, Taipei, Taiwan, ROC, Nov. 2002, IEEE, vol. 2, pp. 1026–1030.